COMMERCIAL WIRELESS METALANGUAGE SCENARIO

Mark Cummings (enVia Technology Partners, Atherton CA; markcummings@envia.com)
Todor Cooklev (San Francisco State University, San Francisco, CA; tcooklev@ieee.org)
Bryan Lyles (Telcordia Technologies, Piscataway NJ; blyles@research.telcordia.com)
P. A. Subrahmanyam (Stanford University, Palo Alto, CA; psubra@ieee.org)

ABSTRACT

In this paper we analyze the current state of multimode cognitive devices and networks, heterogeneous handoff protocols, and trend towards "open access". It is noted that these powerful trends increasingly require a standard mechanism that enables ecosystem participants to communicate in non-traditional ways. Furthermore, we present commercial scenarios that further motivate such a standard. The rationale for an Industry Standard Metalanguage along was recently presented in [1, 9]. The goal of such a metalanguage is to enable a mechanism that provides a standard communication interface to each of the value chain participants on one side and to the radio systems (hardware and software) on the other side. The metalanguage description can contain information about hardware / software functionality / configuration, Air Interface Standards, the information being exchanged, and end users. We discuss characteristics of the metalanguage for standardizing mechanisms for real-time communication of configuration information across a network that supports both legacy and configurable components. These mechanisms allow an element in such a network to determine the range of capabilities of a configurable node, and/or to request specific functionality.

1. INTRODUCTION & BACKGROUND

As a society we are becoming extremely dependant on wireless communications. In most of the developed world, the number of cellular subscribers is larger than the number of wired telephony subscribers. In the developing world, the dependence is even greater. Wireless network architectures that were originally designed to be a high cost convenience add on to reliable wired networks are now being asked to provide reliability beyond five nines with no fall back.

Even as our dependence on them is increasing, our networks are becoming more fragile. Wireless network operators, generally, do not make outages public. Every month or two, one comes to light, but there are likely nine or more outages for every one that comes to light. In order to understand this fragility, it is helpful to look at the situation in similar kinds of networks. Two recent examples are illustrative. Skype was unable to provide service anywhere on the globe for two days. The outage was a result of a software problem. Although it was initially thought to be a problem caused by unexpected behavior of trusted code, there was later speculation that it was caused by a malicious attack. The second example is the collapse of the Wells Fargo network. For two days, one of the large Banks in the US could not operate their ATM's (Automatic Teller machines), Home Banking Services, or any of their web-based services.

The organization of this paper is as follows. In Section 2 we review the current major changes that the wireless industry is undergoing. We draw the conclusion that these changes increasingly call for the use of the proposed metalanguage. Section 3 contains background information on the metalanguage. Since the networks are increasingly heterogeneous, an appropriate handover protocol is required. The recently developed IEEE 802.21 standard supports handoffs among heterogeneous networks. Section 4 examines the path for the adoption of this language. Section 5 contains relevant commercial scenarios. Section 6 contains the conclusions and likely future directions in the development of this technology.

2. TECTONIC SHIFTS IN THE WIRELESS LANDSCAPE

The commercial wireless industry is undergoing a sea change. Some of the factors driving this sea change include:

- Increasing Heterogeneity
- Increasing Fragility While Dependency Is Increasing
- Increasing S/W Content
- Changing Regulatory Models
- Changing Business Models
- Changing Usage Models

The fact that these changes are occurring simultaneously makes their effect profound and dramatic.

When 3G was in its early stage of development in the nineties, it was positioned as the single world wide air interface standard (AIS) that would replace all others. It is clear now that the number of AIS's has increased dramatically, rather than decreasing in number. For example, Japan, a leader in 3G development and deployment, today has the following AIS's currently deployed or in development: PHS, PDC, 1XRTT, UMTS, WiFi, DMB, WiMax, UWB, LTE. At the same time, there is active work going on in Japan surrounding the cognitive radio approach to sharing spectrum between commercial cellular and public safety.

Not only is heterogeneity of AIS's in a network increasing, but there is an increase in heterogeneity within a single AIS. In the past we have seen single AIS's include two different modulation schemes, protocol stacks, and multiple frequency bands, etc. as a mechanism to allow graceful migration. Examples include AMPS, IS-95, and early proposals in Europe for dual mode GSM / UMTS handsets. Now we are seeing much more radical approaches. Many of the Beyond 3G (B3G) proposals are calling for real time switching between completely different modulation schemes. One of these is the LTE (Long Term Evolution) proposal which calls for the simultaneous use of CDMA and OFDM, where CDMA is used for voice and OFDM is used for data. This requires the handset to switch between modulation schemes and the base station to actively reallocate spectrum between the two modulation schemes depending on load.

Another force driving heterogeneity is the global wireless adoption pattern. After thirty years of cellular growth the yearly market for handsets is approaching one billion units a year. WiFi started later, but is showing signs that it may catch up. WiMax is around the corner. Some users replace their wireless devices every six months, while others keep their devices for several years. At the same time, the size of the market attracts new participants. The result is that even after periods of consolidation, new entrants appear and the number and variety of semiconductor and software and hardware component providers increases. The result is that the variety of deployed devices is very large and growing. Now that software download has become common, devices in the field may not be what they were when they left the distribution channel. In-field hardware modification is becoming possible through the use of small format card slots. Given all of this, it is possible today for a one million subscriber network to have 100,000 configurations of devices in the field.

The S/W content in wireless devices, even in the handsets produced by major manufacturers who says that they "only build hardware radios" is increasing. At the same time, S/W centric vendors such as Apple and Google have or are on the verge of entering the industry. The increase in S/W content, is increasing the flexibility and processing power of radios, whether or not an implementation is deemed to be a "full" SDR (Software Defined Radio) This flexibility, combined with the dramatic growth in the number of wireless subscribers / users and the increasing bandwidth demands generated by web access, downloads, etc. are putting pressure on available spectrum. Data rate requirements are increasing faster than the ability of signal processing technology to deliver increases in spectral efficiency, i.e. there is increasing demand for spectrum.

In turn, regulators are responding to the increase in demand for spectrum, in part, by seeking improvements in spectral efficiency, by taking advantage of the increase in flexibility and processing power, and with new regulatory paradigms. The initial focus for improvements in spectral efficiency is on cognitive radio methods. These cognitive radio methods improve spectral efficiency by allowing radios to reconfigure themselves to move into temporarily unused spectrum that they would not otherwise be able to use. The FCC has authorized cognitive radio technology and other administrations around the world are actively considering it.

Recently, attention has started to focus on cognitive networking, sometimes called Knowledge-Based Networking (KBN). Cognitive networks are reconfigured by changing topologies, channel allocation, band mix, AIS mix, etc. Technical work on cognitive networking has been underway in LTE standards effort, E2R and DARPA.

Along with the development of cognitive systems and networks, the spectrum auction process is evolving to spectrum brokerage. In the switch from analog to digital TV broadcasting in the US, spectrum around 700 MHz was freed up for other services. Of this spectrum blocks A (698-704 and 728-734 MHz), B (704-710 and 734-740 MHz), E (722-728 MHz), C (746-757 MHz and 776-787 MHz), and D (758-763 MHz and 788-793 MHz) remain to be licensed; other blocks were auctioned off previously. The US Congress directed the FCC to auction 62 MHz of this returned "analog broadcast spectrum" and allocate 24 MHz to public safety (763-775 MHz) and (793-805 MHz). This auction will take place in January 2008 and is the last major spectrum auction in the foreseeable future. These frequency bands have very favorable signal propagation characteristics both outdoors and indoors, and line-of-sight is not typically required. For example, compared with systems operating at 1900 MHz with wavelength λ_2, at the same transmit power, according to the RF propagation model the average received power will be $10\log_{10}(\lambda_1/\lambda_2)^2$ or approximately 8.5 dB higher for the 700 MHz-based system with wavelength λ_1. This translates into larger coverage

area for every base station and allows a lower cost nationwide network. Therefore systems using this frequency band will be able to offer service that is cheaper than what other wireless systems can offer.

The rules of previous auctions have allowed the licensees, i.e. the incumbent wireless service providers, to block others from entering their market. The conditions for this auction, in particular whether licensee-holders should sub-license the band to other companies generated significant debate. In what attracted significant public attention, Google said it plans to bid at the auction only if the FCC rules require the winner of the auction to sub-lease spectrum to any company under the "open access" rule, i.e. spectrum must be affordably priced and offered on a non-discriminatory basis. Google also wants the auction rules to allow any device and any application to be used on the spectrum. There is an analogy to what is being proposed. Prior to a 1968 FCC ruling, AT&T, then a monopoly for wired telephone service, refused to allow devices not manufactured by it to connect to the telephone network. At present, spectrum licensee-holders in the United States do not allow access to their networks by devices not specifically approved by them. Clearly, allowing access by any device will increase the number of configuration of devices, i.e. the heterogeneity of networks. Technology companies generally support the open access rules, because they anticipate this would increase spending on equipment.

In a very recent decision the FCC accepted partially the request by Google and others and ruled in favor of open access to devices and applications in the 22 MHz-wide C band (746-757 MHz and 776-787 MHz). This would allow consumers to use a handset of their choice and download and run applications of their choice, subject to certain reasonable network management restrictions to protect the network from harm. The licensees of the D band and the public safety band will form a Public Safety/Private Partnership to develop a shared nationwide network for use by both commercial and public safety users, using what is essentially a cognitive radio technology. However, the FCC did not require licensees to wholesale sub-lease spectrum, as advocated by Google. Although not required, spectrum resale appears to be possible. Spectrum brokerage firms are being organized in expectation of this being finalized.

As might be expected an FCC decision of such importance is not without controversy. Verizon is suing the FCC in court claiming that the ruling "violates the U.S. constitution". In spite of the objections of some of those with vested interests, this FCC decision is likely to be the direction of the future. This decision is being closely followed by regulatory administrations around the world. Several appear to be actively preparing for similar actions.

At the time of this writing, it appears that Google will bid in the 700 MHz auction and there is speculation that Apple will also bid. What appears likely to evolve is a system of real time auctions of wholesale spectrum to network operators. Network operators can then respond to changes in usage demand by a combination of cognitive networking and real time purchase or sale of spectrum. In order to make this practical, the underlying decision processes must be automated.

All of these developments form the foundation for a move to end-user centric networks. Just as the network operator makes decisions in real time, in a user centric network, the user's device makes real time decisions on which networks and services to use. Here again, to make this practical, the end user needs to only be required to input high level objectives. Automated processes in the end user's device will make the real time decisions based on a number of dynamic factors, including information provided by:

- The end user
- The end user's behavior patterns
- The end user's types of information
- The types of services available (combination of network operator and regulator information)

3. THE METALANGUAGE

The flexibility of modern wireless systems and the emerging commercial market requires description techniques for identifying the objects in the wireless system universe, their configurations and capabilities, and the services that the users are requesting. . Here, we use the term Metalanguage to mean a system for describing the current configuration of a radio and therefore its current functionality, its potential configuration / functionality; the characteristics of current and potential waveforms and Air Interface Standards (AIS's), the type of information being handled and the type of end users involved. In a world with small numbers of radio types, modes of operation, end-user services, and simple, fixed economic relationships between carriers the construction of formal descriptions is overkill. In the emerging wireless world discussed above and highlighted in the Scenarios Section below, such a metalanguage is critical to achieve the objectives of all roles in the value chain. Large numbers, combined with heterogeneity and compounded by the fact that when a customer moves across networks there is no longer a single network provider make it difficult to impossible for the network to keep a database of "the" configuration." In this new world the programmer has lost the ability to anticipate and correctly code for innovations in configurations and services.

Description of a system is not without tradeoffs. In a short story Jorge Luis Borges imagines a country whose leading cartographers make a map with a 1 to 1 scale to the actual landscape and thereby makes a literary comment on the tradeoff between descriptive precision and usefulness. The same tradeoff exists for the Metalanguage where

attempting to describe every possible system aspect will result in computation intractability. Pragmatism is required.

There are a number of venues where metalanguage or metalanguage-like issues are being worked: The semantic web ontology efforts, the IEEE 802.21 information service, the E2R Integrated Project (IP) of the 6th Framework Programme of the European Commission, and the Comprehensive Metalanguage Effort underway in the SDR Forum Commercial Working Group.

The ability of web browsers to bring a lot of information instantly to the user has had remarkably positive impacts on society. Unfortunately, Key Word Searching algorithms have a tendency to yield a very high proportion of irrelevant information. The Semantic Web initiative seeks to increase the proportion of relevant information produced in web searches by use of Ontology based systems. A lot of resources have been directed at this effort yielding a foundation which can be leveraged in developing a global wireless Metalanguage standard.

An ontology is a data model that represents a domain, describes the objects in the domain, the constraints on the objects, and the relationships between the objects. In the radio world these objects will include handsets and their subcomponents such as RF sections, DSPs, and application processors and the capabilities of the components. Constraints will include the antenna capabilities, DSP capabilities, and power amp limits. Beyond handsets we expect the network capabilities technical specifications and service capabilities to described via ontologies.

A system that can make full use of the flexibility of modern wireless systems must be able to identify the specific applicable objects in its domain description when confronted with a particular request for service, handset. For example, it must be able to match a request for bandwidth against service providers and handset capabilities. Candidates for supporting this feature of the Metalanguage include Description Logics, subsets of first order logic that efficiently model classes of objects. An example of description logic from the Semantic Web community is the Web Ontology Language OWL-DL. Depending on the degree of exactitude needed in the representation, larger subsets of first order logic may be needed, but at the possible cost of computational tractability.

In addition to modeling the objects in the radio world, the metalanguage must provide a protocol for exchanging information about the supported objects and for resolving conflicts when capabilities and requests do not match. The negotiation language allows parties to state their requirements and capabilities and find shared operating regions. The messages associated with the protocol exchanges can be modeled using OWL-DL.

IEEE 802.21 has emerged as a standard for handover services [10] supporting global mobility. To maintain uninterrupted user connections during handovers across dissimilar networks (different AIS networks), IEEE 802.21 defines a common media independent handover (MIH) function between Layer 2 and Layer 3 of the OSI (Open Systems Interconnection) network stack, which facilitates the management and coordination of multiple MAC layers during network mobility events.

In addition to its link layer services, IEEE 802.21 defines an information service. The Media Independent Information Service (MIIS) provides a framework by which a handover function may discover and obtain network information to facilitate handovers. In particular, the Media Independent Information Service defines various network and service associated Information Elements (vocabulary describing objects) and provides an information retrieval service that allows queries to be made against the database. Using the information service a network element or a mobile can discover the nearby networks, their configuration parameters, capabilities, and policies.

E^2R has been working on FDL (Function Description Language). It is similar to 802.21 in area of focus. It seeks to allow devices to communicate a standard description of their functionality.

The SDR Forum Commercial Working Group has been focusing on harmonizing these efforts and extending them to include being able to describe semiconductors, components, subsystems, systems, types of information and types of users. The Working Group has been in liaison with a number of other standards groups and industry organizations seeking to insure that what comes out of everyone's efforts is a single global standard which meets all of the needs rather than a variety of balkanized incompatible standards.

4. COMMERCIAL SCENARIOS

The development of a global standard metalanguage has focused on emerging industry requirements after devices are fielded. However, there are time-to-market and efficiency benefits for industry participants involved in the development, regulatory and distribution channels. This discussion will focus on the later portions of device life cycles. We will focus on three areas in the following order:

- Network configuration and migration
- End User centricity
- System Security

Consider a scenario, where a sporting event is being held at a stadium in an urban core. It is expected that one of the participants will be breaking a long held and honored record. 60,000 people are expected to be in the stadium. Another 10,000 are expected to congregate outside the stadium. There will be 1,000 public safety officials posted

to the stadium and its immediate area to service these crowds. Of the 70,000 people in the crowd, 55,000 are expected to be carrying cell phones. 30% of the cell phones will likely have video camera capability. 20% of the phones will have DMB (video receive). 60% will have still cameras. 90% will have SMS. 30% will have MMS. 25% will have full internet access (10% with modest two way data bandwidth, 10% with medium speed to the handset and modest bandwidth to the base station, and 5% with medium bandwidth in both directions). Additionally there are likely to 40,000 WiFi, and 20,000 WiMax devices. Many of the WiFi and WiMax devices will have VOIP capability. Some portion of these WiFi and WiMax devices will be combination cell phones and some will be additional devices carried by people who also carry a cell phone. Some of the devices that have internet access are IPTV users. There are three network operators providing service in this area. The network operator we are focusing on has licenses in the DMB, Cellular, PCS and WiMax bands; WiFi hotspots (two bands) covering some or all of the stadium (depending on traffic load, population density and positioning of temporary structures in the stadium. The operator also has access through brokers to 700MHz spectrum which can be used. The network operator has roaming agreements, and some fraction of the people attending are expected to be subscribers to other providers and roaming on this network. In addition, there are WiFi access points in the area that are open to the public and not part of a network operator's hotspot service. Some of these access points may be operated by local businesses, others by metropolitan networks.

Some of the people attending will be both watching the live action and watching special video / etc, coverage via DMB or IPTV. At the time of the record breaking event, many of the attending people will call friends, send SMS's, MMS's, emails, etc., send still photos, and send video clips.

In addition to the wide array of device types outlined above, there will be a wide array of subscription types amongst the network's subscribers. Many subscriber devices will have capabilities that have not been activated because the subscriber has not subscribed to the subscription which uses them, they may be locked out, they may need additional S/W downloads to be activated.

The network operator can make some assumptions about the number and types of subscribers, subscriptions, and devices that will be active in and around the stadium. Based on those assumptions, the network operator can develop a strategy such as moving all video phones to WiMax, moving all still camera phones to WiFi, and moving all non video / non camera phones to cellular. Based on this strategy, the network operator can use information gathered from the devices as they arrive, using the metalanguage description and interface. If capacity appears to be insufficient, the network operator can start reconfiguring devices to move to AIS's that they would not normally be able to access, and start bidding on 700 MHz spectrum.

Now we get to the period when capacity demand is peaking, driving a significant portion of the 700MHz brokered spectrum to be in use, and there is an explosion and fire in the immediate vicinity of the stadium. The 700MHz spectrum is claimed by first responders, the remaining brokered spectrum dramatically increases in cost and the network operator has to reconfigure the commercial network. The metalanguage is used again to support network reconfiguration and to the extent necessary, triage. Triage steps, may include restricting WiFi and WiMax bandwidth to effectively shut off VOIP.

There is an additional level of complication. The migration from 2.5 G / 3.0G to B3G such as LTE is going to be happening soon. Now we add this migration process to the above scenario. Another piece of the recent 700MHz decision points to a movement away from network operator centric networks to user centric networks in allowing users to choose devices without operator authorization. Today, some parts of the world are further along in this process than others.

Currently, we are in the midst of a transition from network centric to user centric models. Users today can sign up at a hot spot for a single hour of service. Businesses are deploying not fee for service WiFi networks. Combinations of Cellular, WiFi, WiMax, and Ultra Wideband technologies in single devices will combine with regulatory initiatives, accelerate this process.

In a fully user centric model, users tell their devices what their desires (cost, timeliness, security, etc.) are and intelligence in the device interacts with all the available networks and observations of the user's behavior, etc. to decide on a session by session basis which AIS / service to use. As a radio moves between AIS's, services, networks and operators, it may change its configuration. Therefore, when a device requests service from a particular network, its configuration and range of reconfigurability will not be known by that network, even if it was serviced by that network a short time previously. The metalanguage will allow radios to negotiate with networks on a session by session basis.

As devices become less defined and controlled by a single network operator, increasing emphasis will be placed on security. Also, the increase in the heterogeneity of devices in networks discussed above in combination with the increasing use of s/w downloads driven by bug fixes, addition of new services and real time device reconfiguration is adding to the fragility of wireless networks discussed in section #1 above. These types of problems can occur as a result of system and operational failures as well as security breaches. The best path to

protecting from all of these threats is a three pronged approach, all software to be introduced into a system have:

- A cryptographically protected certification tag that identifies the source of the code
- A MAC (Message Authentication Code – a standard mechanism for producing an encrypted hash of the code)
- A cryptographically protected Metalanguage description of the code

All network elements would contain a protection engine that would check arriving code first for its certification tag. If it came from an acceptable source the engine would move onto the second step – testing the MAC to confirm that the code had not been modified in transmission. If that test was positive, the engine would move onto the third stage.

In the third and final stage, the engine would process the incoming code's Metalanguage Description (MLD) in the context of the existing device's hardware/software MLD to determine the likely outcome of introduction of the code. If the result is positive, the new code would be marked for installation and placed in the approved library. If not a message would be sent to the source of the code informing the source that it is not acceptable. When conditions merit the installation of the approved code, a test is performed to first determine if the system configuration has changed since the last test. If the configuration has changed, the above process would be repeated. Otherwise the new code would be installed. If any unexpected events transpire after installation of the new code, these would be logged and the log stored with the new code in the library.

It is possible to have the engine remote from the device, however, this adds additional complexity to the process. The most notable source of complexity is that the link between the remote engine and the device must be secured. Other questions surround latency and the ability of the remote engine to have the fully correct current configuration of the device.

5. CONCLUSIONS AND LIKELY FUTURE DIRECTIONS

In this paper we analyze the significant changes currently altering the wireless landscape. These changes include the availability of multimode cognitive devices and networks, heterogeneous handoff protocols, and trend towards "open access". It is noted that these powerful trends increasingly call for the use of a metalanguage, adopted by all participants of the wireless value chain. Several metalanguage related standards efforts are underway. These efforts, focus on pieces of the problem, pointing the way to a comprehensive solution. Value chain participants include: Network Operators, Equipment Vendors, Software Vendors, Semiconductor Vendors, Component Vendors, Regulators and End Users. This metalanguage was proposed earlier in [1, 9]. This metalanguage is the mechanism that provides an interface to each of the value chain participants on one side and to the radio systems (hardware and software) on the other side. The metalanguage contains information about hardware / software functionality / configuration, Air Interface Standards, the information being exchanged, and end users. It is important that this metalanguage be standardized in a way that is not perceived as being biased by any of the various players. In the paper we present commercial scenarios that further motivate such a standard. We discuss characteristics of the metalanguage standardizing mechanisms for real-time communication of configuration information across a network that supports both legacy and configurable components. Therefore the metalanguage allows an element in such a network to determine the range of capabilities of a configurable node, and/or to request specific functionality.

The full value of wireless systems and its cognitive extensions will be achieved when they can autonomously fully meet the goals and objectives of all participants in the wireless value chain across the entire life cycle. The metalanguage significantly facilitates this objective.

6. REFERENCES

[1] M. Cummings and P.A.Subrahmanyam, "The Role of a Metalanguage in the Context of Cognitive Radio Lifecycle Support, SDR Forum Technical Conference, 2006.

[2] European Telecommunications Standards Institute, http://www.etsi.org

[3] International Telecommunications Union, http://www.itu.int

[4] Open Mobile Alliance, http://www.openmobilealliance.org

[5] Resource Description Framework, http://www.w3.org/RDF/

[6] W3C RDF Validation service, http://www.w3.org/RDF/Validator/

[7] Unified Modelling Language, http://www.uml.org

[8] Commercial Handset Guidelines, Technical Report TR2.1, SDR Forum, http://sdrforum.org

[9] P.A.Subrahmanyam and Mark Cummings, "Perspectives on a Metalanguage for Configurable Wireless Systems," SDR Technical Conference 2004.

[10] IEEE 802.21 Working Group, http://www.ieee802.org/21